

Addition law structure of elliptic curves

David Kohel

Institut de Mathématiques de Luminy
 Université de la Méditerranée
 163, avenue de Luminy, Case 907
 13288 Marseille Cedex 9
 France

Abstract

The study of alternative models for elliptic curves has found recent interest from cryptographic applications, after it was recognized that such models provide more efficiently computable algorithms for the group law than the standard Weierstrass model. Examples of such models arise via symmetries induced by a rational torsion structure. We analyze the module structure of the space of sections of the addition morphisms, determine explicit dimension formulas for the spaces of sections and their eigenspaces under the action of torsion groups, and apply this to specific models of elliptic curves with parametrized torsion subgroups.

1 Introduction

Let k be a field and A an abelian variety over k with a given projectively normal embedding $\iota : A \rightarrow \mathbb{P}^r$, determined by an invertible sheaf $\mathcal{O}_A(1) := \iota^* \mathcal{O}_{\mathbb{P}^r}(1)$ and denote the addition morphism on A by $\mu : A \times A \rightarrow A$.

An *addition law* is an $(r+1)$ -tuple $\mathfrak{s} = (p_0, \dots, p_r)$ of bihomogeneous elements p_j of

$$k[A] \otimes k[A] = k[X_0, \dots, X_r]/I_A \otimes_k k[X_0, \dots, X_r]/I_A,$$

where I_A is the defining ideal of A , such that the rational map

$$(x, y) = ((x_0 : \dots : x_r), (y_0 : \dots : y_r)) \mapsto (p_0(x, y) : \dots : p_r(x, y))$$

defines μ on the complement of $Z = V(p_0, \dots, p_r)$ in $A \times A$. The set Z is called the *exceptional set* of \mathfrak{s} . Lange and Ruppert [16] give a characterization of addition laws, as sections of an invertible sheaf, from which it follows that the exceptional set of any nonzero addition law is the support of a divisor, which we refer to as the *exceptional divisor*. An addition law is said to have bidegree (m, n) if $p_j(x, y)$ are homogeneous of degree m and n in x_i and y_j , respectively. The addition laws of bidegree (m, n) , including the zero element, form a k -vector space.

A set S of addition laws is said to be *complete* or *geometrically complete* if the intersection of the exceptional sets of all \mathfrak{s} in S is empty, and *k-complete* or *arithmetically complete* if this intersection contains no k -rational point. We note that the term *complete* [6, 16, 17] has more recently been used to denote k -complete, in literature with a view to computational and cryptographic application. The intersection of the exceptional sets for \mathfrak{s} in S clearly equals the intersection of the exceptional sets for all \mathfrak{s} in its k -linear span.

The structure of addition laws depends intrinsically not just on A , but also on the embedding $\iota : A \rightarrow \mathbb{P}^r$, determined by global sections s_0, \dots, s_r in $\Gamma(A, \mathcal{L})$, for the sheaf $\mathcal{L} = \mathcal{O}_A(1)$. The hypothesis that ι is a projectively normal embedding may be defined to be the surjectivity of the homomorphism

$$k[X_0, \dots, X_r] = \bigoplus_{n=0}^{\infty} \Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(n)) \longrightarrow \bigoplus_{n=0}^{\infty} \Gamma(A, \mathcal{L}^n)$$

(see Birkenhake-Lange [5, Chapter 7, Section 3] or Hartshorne [10, Chapter I, Exercise 3.18 & Chapter II, Exercise 5.14]). In particular, it implies that $\{s_0, \dots, s_r\}$ span $\Gamma(A, \mathcal{L})$. For an elliptic curve, the surjectivity of $\Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(1))$ on $\Gamma(E, \mathcal{L})$ is a necessary and sufficient condition for ι to be projectively normal. We recall that an invertible sheaf is said to be *symmetric* if $\mathcal{L} \cong [-1]^* \mathcal{L}$. Lange and Ruppert [16] determine the structure of addition laws, and in particular prove the following main theorem.

Theorem 1 (Lange-Ruppert) *Let $\iota : A \rightarrow \mathbb{P}^r$ be a projectively normal embedding of A , and $\mathcal{L} = \mathcal{O}_A(1)$. The sets of addition laws of bidegrees $(2, 3)$ and $(3, 2)$ on A are complete. If \mathcal{L} is symmetric, then the set of addition laws of bidegree $(2, 2)$ is complete, and otherwise empty.*

Remark. Lange and Ruppert assume that ι is defined with respect to the complete linear system of an invertible sheaf $\mathcal{L} \cong \mathcal{M}^m$ where \mathcal{M} is ample and $m \geq 3$. Their hypothesis implies the projective normality of ι by a result of Sekiguchi [21] and the latter is sufficient for their proof. Following Sekiguchi, Lange and Ruppert require that k be algebraically closed, but the result relies only on the dimensions of sections of a certain line bundle and base-point freeness of its sections, which are independent of the base field. We avoid this dependence by the direct assumption that ι is projectively normal.

Bosma and Lenstra [6] give a precise description of the exceptional divisors of addition laws of bidegree $(2, 2)$ when A is an elliptic curve embedded as a Weierstrass model. Using this analysis, they prove that two addition laws are sufficient for a complete system. However, their description of the structure of addition laws applies more generally to other projective embeddings of an elliptic curve. We carry out this analysis to determine the dimensions of spaces of addition laws in families with rational torsion subgroups and study the module decomposition of these spaces with respect to the action of torsion.

In view of Theorem 1, the simplest possible structure of an addition law we might hope for is one for which the polynomials $p_j(x, y)$ are binomials of bidegree

(2, 2). Such addition laws are known for Hessian models [8, Section 4], [13], [22], Jacobi quadric intersections [8, Section 4], and for Edwards models [1], [9] of elliptic curves. After recalling some background in Sections 2 and 3, and proving results about the exceptional divisors of addition laws, we introduce the concept of addition law projections in Section 4. In Section 5 we introduce the notion of a projective normal closure of an affine model of an elliptic curve in order to apply the preceding theory. Section 6 gives a formal definition and interpretation of affine addition laws, expressed by rational functions, in terms of the addition law projections of Section 4. In Section 7 we introduce a G -module structure of addition laws, with respect to a rational torsion subgroup on E . In the final section we give examples of addition laws, observing that the simple laws coincide with the uniquely determined one-dimensional eigenspaces for the G -module structure. In the final section we analyze the G -module structure of addition laws for standard families – the degree 3 twisted Hessian models, the Jacobi quadric intersections and twisted Edwards models of degree 4 – and construct an analogous degree 5 model for curves with a rational 5-torsion structure.

2 Divisors and invertible sheaves on abelian varieties

Let A/k be an abelian variety. We denote the addition morphism by μ , the difference morphism by δ , and let $\pi_i : A \times A \rightarrow A$ be the projection maps, for i in $\{1, 2\}$. We denote by μ^* , δ^* , and π_i^* the respective pullback morphisms of divisors and sheaves from E to $E \times E$.

We use the bijective correspondence between Weil divisors and Cartier divisors on abelian varieties, and to such a divisor D we associate an invertible subsheaf $\mathcal{L}(D)$ of the sheaf \mathcal{K} of total quotient rings such that for D effective, $\mathcal{L}(D)^{-1}$ is the ideal sheaf of D (see Hartshorne [10, Chapter II, Section 6]). We call the invertible sheaf \mathcal{L} *effective* if it is isomorphic to $\mathcal{L}(D)$ for some effective divisor D .

For $\mathcal{L}(D)$ so defined, its space of global sections is the Riemann-Roch space:

$$\Gamma(A, \mathcal{L}(D)) = \{f \in k(A) : \operatorname{div}(f) \geq D\},$$

and an embedding $A \rightarrow \mathbb{P}^r$ given by the complete linear system $|\mathcal{L}(D)|$ is determined by

$$P \mapsto (x_0(P) : x_1(P) : \cdots : x_r(P)),$$

for a choice of basis $\{x_0, x_1, \dots, x_r\}$ of $\Gamma(A, \mathcal{L}(D))$. If D is an effective Weil divisor we may take $x_0 = 1$, in which case we recover D as the intersection with the hyperplane $X_0 = 0$ in \mathbb{P}^r .

2.1 Sheaves associated to the addition morphism

Lange and Ruppert [16] interpret an addition law of bidegree (m, n) as a homomorphism of sheaves $\mu^* \mathcal{L} \rightarrow \pi_1^* \mathcal{L}^m \otimes \pi_2^* \mathcal{L}^n$, then use the identification

$$\mathrm{Hom}(\mu^* \mathcal{L}, \pi_1^* \mathcal{L}^m \otimes \pi_2^* \mathcal{L}^n) = \Gamma(A \times A, \mu^* \mathcal{L}^{-1} \otimes \pi_1^* \mathcal{L}^m \otimes \pi_2^* \mathcal{L}^n),$$

to determine their structure. In view of Theorem 1, we will be interested in symmetric invertible sheaves \mathcal{L} , and the structure of sections of the sheaves

$$\mathcal{M}_{m,n} = \mu^* \mathcal{L}^{-1} \otimes \pi_1^* \mathcal{L}^m \otimes \pi_2^* \mathcal{L}^n.$$

and for the critical case of $\mathcal{M}_{2,2}$ we write more concisely \mathcal{M} .

We return to the study of sheaves on $E \times E$ after characterizing certain properties of invertible sheaves and morphisms of elliptic curves.

2.2 Invertible sheaves on elliptic curves

A Weierstrass model of an elliptic curve E with base point O is determined with respect to $\mathcal{L}(3(O))$ and any other cubic model in \mathbb{P}^2 is obtained as a projective linear automorphism of the Weierstrass model. As a prelude to the study of models determined by more general symmetric divisors, we recall the characterization of divisors on an elliptic curve. For a divisor D on an elliptic curve let $ev(D)$ be its evaluation on the curve. With this notation, the following lemma is immediate.

Lemma 2 *Let $\mathcal{L} = \mathcal{L}(D)$ be an invertible sheaf of degree d on E . Then $\mathcal{L} \cong \mathcal{L}((d-1)(O) + (P))$ where $P = ev(D)$. Moreover \mathcal{L} is symmetric if and only if P is in $E[2]$.*

The classification of curves and their addition laws makes use of linear isomorphisms between spaces of global sections of an invertible sheaf. In classifying curves and their addition laws, it therefore makes sense to classify elliptic curves up to projective linear isomorphism.

Lemma 3 *Let E_1 and E_2 be projectively normal embeddings of an elliptic curve E defined with respect to divisors D_1 and D_2 . Then there exists a projective linear isomorphism $E_1 \rightarrow E_2$ if and only if $\deg(D_1) > \deg(D_2)$ or $D_1 \sim D_2$.*

Proof An equivalence of divisors $D_1 \sim D_2$ implies $\mathcal{L}(D_1) \cong \mathcal{L}(D_2)$, and the resulting linear isomorphism of global sections induces a linear isomorphism of the embeddings of the curve with respect to D_1 and D_2 (and whose inverse is also linear). If $\deg(D_1) > \deg(D_2)$, we may suppose – up to equivalence – that $D_1 > D_2 > 0$, and we have an inclusion of vector subspaces of $k(E)$:

$$V_2 = \Gamma(E, \mathcal{L}(D_2)) \subseteq V_1 = \Gamma(E, \mathcal{L}(D_1))$$

such that the restriction from V_1 to V_2 determines the morphism $E_1 \rightarrow E_2$ induced by a surjective linear map on coordinate functions. Since V_2 defines the embedded image E_2 , the restriction morphism is an isomorphism. \square

A symmetric embedding gives rise to addition laws of minimal bidegree in Theorem 1. However, the structure of the negation map imposes additional motivation for requiring a symmetric line bundle.

Lemma 4 *If $E \subset \mathbb{P}^r$ is a projectively normal embedding with respect to \mathcal{L} , then $[-1]$ is induced by a projective linear automorphism if and only if \mathcal{L} is symmetric.*

Proof If \mathcal{L} is symmetric, then $[-1]^*$ induces an automorphism of the space of global sections of \mathcal{L} . Conversely, since E is projectively normal in \mathbb{P}^r , a linear automorphism of the coordinate functions which determines $[-1]$ also induces an automorphism of global sections, hence of \mathcal{L} with $[-1]^*\mathcal{L}$. \square

In Section 7 we analyze the G -module structure of addition laws with respect to a finite subgroup $G = \{T_i\}$ of rational points on E . For a rational point T of E we denote by τ_T the translation-by- T map on E . The following lemma characterizes when τ_T acts linearly.

Lemma 5 *Let $E \subset \mathbb{P}^r$ be a projectively normal embedding with respect to \mathcal{L} , and let T be in $E(k)$. Then τ_T is induced by a projective linear automorphism if and only if $[\deg(\mathcal{L})]T = O$.*

Proof It is necessary and sufficient to show that $\mathcal{L} \cong \tau_T^*\mathcal{L}$. Let $\mathcal{L} \cong \mathcal{L}(D)$ and set $D' = \tau_T^*D$. Since $\deg(D') = \deg(D)$ and $ev(D') = ev(D) - [\deg(D)]T$, by the canonical form of Lemma 2 the equivalence of the isomorphism $\mathcal{L} \cong \tau_T^*\mathcal{L}$ holds if and only if $[\deg(D)]T = O$. \square

Remark. We note that Lemma 3 and Lemma 4 refer to isomorphisms in the category of elliptic curves (fixing a base point), while the isomorphism of Lemma 5 is not an elliptic curve isomorphism. Lemma 3 is false if an isomorphism in the category of curves is allowed. Suppose that E_1 and E_2 are embedded with respect to divisors D_1 and D_2 and that $D_1 \sim \tau_T^*D_2$. Then the morphism τ_T determines a linear isomorphism $E_1 \rightarrow E_2$ sending O to T .

2.3 Invertible sheaves on $E \times E$

Let μ , δ , π_1 , and π_2 be the addition, difference, and projection morphisms, as above. We define

$$V = \{O\} \times E \text{ and } H = E \times \{O\}$$

as divisors on $E \times E$. Similarly, let Δ and ∇ be the diagonal and anti-diagonal images of E in $E \times E$, respectively.

Lemma 6 *With the above notation we have*

$$\begin{aligned} \pi_1^*\mathcal{L}((O)) &= \mathcal{L}(V), & \pi_2^*\mathcal{L}((O)) &= \mathcal{L}(H), \\ \mu^*\mathcal{L}((O)) &= \mathcal{L}(\nabla), & \delta^*\mathcal{L}((O)) &= \mathcal{L}(\Delta). \end{aligned}$$

In particular if $\mathcal{L} = \mathcal{L}(d(O))$, then

$$\mu^*\mathcal{L}^{-1} \otimes \pi_1^*\mathcal{L}^m \otimes \pi_2^*\mathcal{L}^n = \mathcal{L}(-d\nabla + dmV + dnH).$$

Proof This is immediate from

$$V = \pi_1^*(O), \quad H = \pi_2^*(O), \quad \nabla = \mu^*(O) \text{ and } \Delta = \delta^*(O). \quad \square$$

We note that each of V , H , ∇ , and Δ is an elliptic curve isomorphic to E . In the generalization of the divisor on E from $3(O)$ to a more general Weil divisor, we obtain translates of these elementary divisors, which motivates the definitions

$$\begin{aligned} \nabla_P &:= \mu^*(P) = \nabla + (P, O) = \nabla + (O, P), & V_P &:= \pi_1^*(P) = V + (P, O), \\ \Delta_P &:= \delta^*(P) = \Delta + (P, O) = \Delta - (O, P), & H_P &:= \pi_2^*(P) = H + (O, P). \end{aligned}$$

For points Q and R in $E(\bar{k})$, let τ_Q and $\tau_{(Q,R)}$ be the translation morphisms on E and $E \times E$. The following lemma is immediate from the definitions.

Lemma 7 *The translation morphism $\tau_{(Q,R)}$ on $E \times E$ acts by pullback on divisors by:*

$$\begin{aligned} \tau_{(Q,R)}^*(\Delta_P) &= \Delta_{P-Q+R}, & \tau_{(Q,R)}^*(V_P) &= V_{P-Q}, \\ \tau_{(Q,R)}^*(\nabla_P) &= \nabla_{P-Q-R}, & \tau_{(Q,R)}^*(H_P) &= H_{P-R}. \end{aligned}$$

2.4 Addition laws of bidegree $(2, 2)$

We now classify the sheaves of addition laws of bidegree $(2, 2)$. We recall the definition of the invertible sheaf

$$\mathcal{M} = \mu^* \mathcal{L}^{-1} \otimes \pi_1^* \mathcal{L}^2 \otimes \pi_2^* \mathcal{L}^2.$$

Following Bosma and Lenstra [6], we let x be a degree 2 function on E with poles only at O , and observe that for $x_1 = x \otimes 1$ and $x_2 = 1 \otimes x$ in $k(E) \otimes_k k(E) \subset k(E \times E)$, we have

$$\operatorname{div}(x_1 - x_2) = \nabla + \Delta - 2V - 2H.$$

This relation gives rise to the following more general systems of relations.

Lemma 8 *For points P and Q in $E(\bar{k})$ we have*

$$\Delta_{P-Q} + \nabla_{P+Q} \sim V + V_{2P} + H + H_{2Q}.$$

If T_1 and T_2 are in $E[2]$ and $T_3 = T_1 + T_2$, we have

$$\Delta_{T_1} + \nabla_{T_2} \sim V + V_{T_3} + H + H_{T_3}.$$

Proof The first relation is the homomorphic image of $\nabla + \Delta \sim 2V + 2H$ under $\tau_{(P,Q)}^*$, applying Lemma 7, then using the equivalences $2V_P \sim V + V_{2P}$ and $2H_P \sim H + H_{2P}$, which follow from the pullbacks of the sheaf isomorphisms of Lemma 2. The second relation follows by taking S_1 and S_2 such that $2S_i = T_i$, and specializing to $(P, Q) = (-S_1 + S_2, S_1 + S_2)$. \square

The above lemma yields the following isomorphisms in terms of symmetric invertible sheaves.

Lemma 9 *Let \mathcal{L} be a symmetric invertible sheaf on E , let T_1 and T_2 be points in $E[2]$ and set $T_3 = T_1 + T_2$. The sheaves $\mathcal{L}_i = \tau_{T_i}^*(\mathcal{L})$ satisfy*

$$\mu^* \mathcal{L}_1 \otimes \delta^* \mathcal{L}_2 \cong \pi_1^* \mathcal{L} \otimes \pi_1^* \mathcal{L}_3 \otimes \pi_2^* \mathcal{L} \otimes \pi_2^* \mathcal{L}_3,$$

and in particular

$$\mu^* \mathcal{L} \otimes \delta^* \mathcal{L} \cong \pi_1^* \mathcal{L}^2 \otimes \pi_2^* \mathcal{L}^2,$$

from which $\mathcal{M} \cong \delta^* \mathcal{L}$.

Proof By Lemma 2, we have $\mathcal{L} \cong \mathcal{L}((d-1)(O) + (T))$ for some point T in $E[2]$, and hence $\mathcal{L}^2 \cong \mathcal{L}(2d(O))$, and similarly for the translates \mathcal{L}_i . The lemma then follows by the equivalences of Lemma 8, extended linearly to the pullbacks of divisors of the form $(d-1)(O) + (T)$. \square

The following theorem extends the analysis of Bosma and Lenstra [6, Section 4], following the lines of proof of Lange and Ruppert [16, Section 2] and [17].

Theorem 10 *Let $\iota : E \rightarrow \mathbb{P}^r$ be a projectively normal embedding of an elliptic curve, with respect to a symmetric sheaf $\mathcal{L} \cong \mathcal{L}(D)$. Then the space of global sections of \mathcal{M} is isomorphic to the space of global sections of \mathcal{L} . Moreover, the exceptional divisor of an addition law of bidegree $(2, 2)$ associated to a section in $\Gamma(E \times E, \mathcal{M})$ is of the form $\sum_{i=1}^d \Delta_{P_i}$ where $D \sim \sum_i (P_i)$.*

Proof In view of Lemma 9, and since δ has integral fibers, we deduce that the difference morphism induces an isomorphism $\delta^* : \Gamma(E, \mathcal{L}) \rightarrow \Gamma(E \times E, \delta^* \mathcal{L})$. The structure of the exceptional divisor follows since for $D \sim \sum_i (P_i)$, we have $\delta^* D \sim \sum_i \Delta_{P_i}$. \square

Since each Δ_{P_i} is isomorphic to E over the algebraic closure of k , this theorem gives a simple characterization of the exceptional divisor, and of arithmetic completeness.

Corollary 11 *The exceptional divisor of an addition law of bidegree $(2, 2)$ is of the form $C = \delta^*(D')$ where $C \cap H = D' \times \{O\}$.*

Proof Each component of C is of the form $\Delta_P = \delta^*(P)$ for a uniquely determined P , and the identity $\Delta_P \cap H = (P, O)$ extends linearly to general sums of divisors of the form Δ_P . \square

Corollary 12 *An addition law of bidegree $(2, 2)$ with exceptional divisor $C = \delta^*(D')$ is k -complete if and only if D' has no k -rational point in its support.*

Proof A component Δ_P of C has a rational point (and is isomorphic to E) if and only if the point P lies in $E(k)$. \square

Remark. For addition laws of bidegree $(2, 2)$, Corollary 11 gives an elementary algorithm for characterizing the exceptional divisor and Corollary 12 for characterizing arithmetic completeness.

3 Divisors and intersection theory

For higher bidegrees, we do not expect to have an isomorphism between the space addition laws and the sections of an invertible sheaf on E . In order to determine the dimensions of these spaces, we require an explicit determination of the Euler-Poincaré characteristic $\chi(E \times E, \mathcal{L})$ as a tool for determining the dimension of $\Gamma(E \times E, \mathcal{L}) = H^0(E \times E, \mathcal{L})$.

3.1 Euler-Poincaré characteristic and divisor equivalence

For a projective variety X/k and a sheaf \mathcal{F} , and let $\chi(X, \mathcal{F})$ be the Euler-Poincaré characteristic:

$$\chi(X, \mathcal{F}) = \sum_{i=0}^{\infty} (-1)^i \dim_k(H^i(X, \mathcal{F})).$$

For the classification of divisors or invertible sheaves of X , we have considered the *linear equivalence* classes in $\text{Pic}(X)$. In order to determine the dimensions of spaces of addition laws, it suffices to consider the coarser *algebraic equivalence* class in the *Néron-Severi group* of X , defined as

$$\text{NS}(X) = \text{Pic}(X)/\text{Pic}^0(X).$$

For a surface X , a divisor D is *numerically equivalent* to zero if the intersection product $C.D$ is zero for all curves C on X . This gives the coarsest equivalence relation on X and we denote the group of divisors modulo numerical equivalence by $\text{Num}(X)$. We refer to Lang [15, Chapter IV] for the general definition of $\text{Num}(X)$, and the equality between $\text{Num}(X)$ and $\text{NS}(X)$ for abelian varieties:

Lemma 13 *If X is an abelian variety then $\text{NS}(X) = \text{Num}(X)$.*

By the definition of numerical equivalence, the intersection product is non-degenerate on $\text{Num}(X)$. In the application to $X = E \times E$, we can determine the structure of $\text{NS}(X)$.

Lemma 14 *The following diagram is exact.*

$$\begin{array}{ccccccc} & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \text{Pic}^0(E) \times \text{Pic}^0(E) & \longrightarrow & \text{Pic}^0(E \times E) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \text{Pic}(E) \times \text{Pic}(E) & \xrightarrow{\pi_1^* \times \pi_2^*} & \text{Pic}(E \times E) & \longrightarrow & \text{End}(E) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \text{NS}(E) \times \text{NS}(E) & \longrightarrow & \text{NS}(E \times E) & \longrightarrow & \text{End}(E) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & 0 & & 0 & & 0 \end{array}$$

Proof Exactness of the middle horizontal sequence is Exercise IV 4.10 of Hartshorne [10], and the vertical sequences are exact by the definition of the Néron-Severi group. Exactness of the upper and lower sequences follows by commutativity of the diagram. \square

We note that since $\text{NS}(E)$ and $\text{End}(E)$ are free abelian groups, the lower sequence splits, with the splitting sending an endomorphism φ to its graph Γ_φ , where, in particular, $\Gamma_{[1]} = \Delta$ and $\Gamma_{[-1]} = \nabla$. Moreover, $E \times E$ is isomorphic to $\text{Pic}^0(E \times E)$, with isomorphism $(P, Q) \mapsto V_P - V + H_Q - H$.

Summarizing arguments from Lange and Ruppert [17], particularly the proof of Lemma 1.3, we now determine the intersection pairing on $\text{NS}(E \times E)$.

Lemma 15 *The Néron-Severi group $\text{NS}(E \times E)$ is a finitely generated free abelian group, and if $\text{End}(E) \cong \mathbb{Z}$, it is generated by V , H , Δ , and ∇ , modulo the relation $\Delta + \nabla \equiv 2V + 2H$. The intersection product is nondegenerate on $\text{NS}(E \times E)$ and given by*

	V	H	Δ	∇
V	0	1	1	1
H	1	0	1	1
Δ	1	1	0	4
∇	1	1	4	0

Proof The divisors V and H are the generators of $\pi_1^*(\text{NS}(E))$ and $\pi_2^*(\text{NS}(E))$. Since Δ and ∇ are the graphs of $[1]$ and $[-1]$, their sum induces the zero homomorphism, thus must lie in the image of $\pi_1^* \times \pi_2^*$. The expression for $\Delta + \nabla$ follows from the linear equivalence relation of Lemma 8. Each of V , H , Δ and ∇ has trivial self-intersection, since they have trivial intersections with their translates in $E \times E$. The identities

$$V.H = V.\Delta = V.\nabla = H.\Delta = H.\nabla = 1,$$

hold since each pair has a unique intersection point (O, O) , and finally $\Delta.\nabla = 4$ follows from $|\Delta \cap \nabla| = |\{(T, T) : T \in E[2]\}| = 4$. \square

In the case of complex multiplication, the generator set can be extended by additional independent divisors $\Gamma_{\varphi_1}, \dots, \Gamma_{\varphi_{r-1}}$, where $\{1, \varphi_1, \dots, \varphi_{r-1}\}$ is a basis for $\text{End}(E)$, by the splitting of the lower sequence of Lemma 14.

Theorem 16 *Let E be an elliptic curve and \mathcal{L} be an invertible sheaf on $E \times E$. The Euler-Poincaré characteristic $\chi(E \times E, \mathcal{L})$ depends only on the numerical equivalence class of \mathcal{L} , and in particular*

$$\chi(E \times E, \mathcal{L}(D)) = \frac{1}{2}D.D.$$

If \mathcal{L} is ample, then $\chi(E \times E, \mathcal{L}) = \dim_k(\Gamma(E \times E, \mathcal{L}))$. Conversely, if \mathcal{L} is effective and $\chi(E \times E, \mathcal{L})$ is positive, then \mathcal{L} is ample.

Proof The first statement is the Riemann-Roch theorem for abelian surfaces (see Mumford [20, p. 150] or Hartshorne [10, Chapter V, Theorem 1.6]). For the latter statements, Mumford's Vanishing Theorem [20, p. 150] states that when $\chi(E \times E, \mathcal{L})$ is nonzero, $H^i(E \times E, \mathcal{L}) \neq 0$ for exactly one $i = i(\mathcal{L})$ and that $0 \leq i \leq 2$. In addition, $i(\mathcal{L}) = i(\mathcal{L}^n)$ for all $n > 0$ [20, Corollary, p. 159]. If \mathcal{L} is ample it follows that $i = 0$, and since $H^0(E \times E, \mathcal{L}) = \Gamma(E \times E, \mathcal{L})$ gives the only contribution to the Euler-Poincaré characteristic, the result follows. In the other direction, for positive Euler-Poincaré characteristic, clearly $i \neq 1$, and by Serre duality [10, Chapter III, Corollary 7.7] we have $i(\mathcal{L}^{-1}) = 2 - i(\mathcal{L})$. For \mathcal{L} effective, $H^0(E \times E, \mathcal{L}^{-1}) = 0$, hence $i = 0$. Ampleness of \mathcal{L} follows by Application 1 of Mumford [20, p. 60]. \square

The following corollary of Theorem 16 and Lemma 15, which is synthesis of results of Lange and Ruppert [16, 17], allows the effective determination of the Euler-Poincaré characteristic.

Corollary 17 (Lange-Ruppert) *Let E be an elliptic curve, then*

$$\chi(E \times E, \mathcal{L}(x_0 \nabla + x_1 V + x_2 H)) = x_0 x_1 + x_0 x_2 + x_1 x_2.$$

In particular, if \mathcal{L} is an invertible sheaf of degree $d > 0$ on E , then

$$\chi(E \times E, \mathcal{M}_{m,n}) = d^2(mn - m - n).$$

As an application, we have a clear criterion for the sheaves $\mathcal{M}_{m,n}$ to be effective and ample. We define the product order in bidegrees by $(k, l) < (m, n)$ if and only if $k < m$ and $l < n$.

Corollary 18 *The sheaf $\mathcal{M}_{m,n}$ is ample if and only if $(2, 2) < (m, n)$.*

Proof The Euler-Poincaré characteristic, $\chi(E \times E, \mathcal{M}_{m,n}) = d^2(mn - m - n)$, is positive if and only if $(2, 2) < (m, n)$ by Corollary 17, and this is a necessary condition for ampleness, e.g. by the Nakai-Moishezon Criterion (see Hartshorne [10, Chapter V, Theorem 1.10]). On the other hand, $\mathcal{M}_{m,n}$ is isomorphic to

$$\mathcal{L}(d\Delta + d(m-2)V + d(n-2)H),$$

hence is effective when $(2, 2) < (m, n)$, so $\mathcal{M}_{m,n}$ is ample by Theorem 16. \square

Next we obtain a characterization of the critical case $\chi(E \times E, \mathcal{L}(D)) = 0$. In view of the roles of ∇ , Δ , V , and H in the divisor theory, we define $\Gamma_{(a,b)}$ to be the image of E in $E \times E$ given by $P \mapsto (aP, bP)$, for a and b coprime, and for (na, nb) set $\Gamma_{(na,nb)} = n^2 \Gamma_{(a,b)}$. We then have equivalent expressions

$$\Delta = \Gamma_{(1,1)}, \quad \nabla = \Gamma_{(1,-1)}, \quad V = \Gamma_{(0,1)}, \quad H = \Gamma_{(1,0)}.$$

Lemma 19 *The divisor $\Gamma_{(a,b)}$ is numerically equivalent to*

$$-ab\nabla + (a^2 + ab)V + (ab + b^2)H.$$

Proof The numerical equivalence class is determined by the intersection products

$$(\nabla.\Gamma_{(a,b)}, V.\Gamma_{(a,b)}, H.\Gamma_{(a,b)}) = ((a+b)^2, b^2, a^2),$$

which agrees with that of the divisor $-ab\nabla + (a^2 + ab)V + (ab + b^2)H$. \square

Theorem 20 *A divisor D on $E \times E$ satisfies $\chi(E \times E, \mathcal{L}(D)) = 0$ if and only if D is numerically equivalent to $n\Gamma_{(a,b)}$ for integers n, a and b .*

Proof By Lemma 15, every divisor is numerically equivalent to one of the form $D = x_0\nabla + x_1V + x_2H$. By Corollary 17, the identity $\chi(E \times E, \mathcal{L}(D)) = 0$ defines a conic

$$C : x_0x_1 + x_0x_2 + x_1x_2 = 0$$

in \mathbb{P}^2 , which has a parametrization $\mathbb{P}^1 \rightarrow C$ given by

$$(a : b) \longrightarrow (-ab : a^2 + ab : ab + b^2),$$

hence every triple (x_0, x_1, x_2) satisfying $x_0x_1 + x_0x_2 + x_1x_2 = 0$ is of the form $n(-ab, a^2 + ab, ab + b^2)$ for integers n, a and b . By Lemma 19, the divisor D is numerically equivalent to $n\Gamma_{(a,b)}$. \square

3.2 Dimensions of spaces of addition laws

We are now in a position to relate the dimension of $\Gamma(E \times E, \mathcal{M}_{m,n})$ to $\chi(E \times E, \mathcal{M}_{m,n})$. As a first step, we recall the statement of the Riemann-Roch theorem for elliptic curves.

Theorem 21 *If \mathcal{L} is an invertible sheaf of degree $d > 0$ on an elliptic curve E , then \mathcal{L} is ample and $\dim_k(\Gamma(E, \mathcal{L})) = d$.*

Corollary 22 *Let \mathcal{L} be a symmetric ample invertible sheaf of degree d on an elliptic curve E and*

$$\mathcal{M}_{m,n} = \mu^* \mathcal{L}^{-1} \otimes \pi_1^* \mathcal{L}^m \otimes \pi_2^* \mathcal{L}^n.$$

Then for $(m, n) = (2, 2)$,

$$\dim_k(H^0(E \times E, \mathcal{M})) = \dim_k(H^1(E \times E, \mathcal{M})) = d,$$

and for all other $m, n \geq 2$,

$$\dim_k(H^0(E \times E, \mathcal{M}_{m,n})) = d^2(mn - m - n).$$

Proof Since $\mathcal{M}_{m,n}$ is isomorphic to $\mathcal{L}(C)$ for an effective divisor C , we have that

$$H^2(E \times E, \mathcal{M}_{m,n}) \cong H^0(E \times E, \mathcal{M}_{m,n}^{-1}) = 0$$

by Serre duality [10, Chapter III, Corollary 7.7], since $\omega_A \cong \mathcal{O}_A$ for any abelian variety A [5, Chapter 1, Lemma (4.2)]. The dimension of the first cohomology

group of $\mathcal{M}_{m,n}$ is then determined by the dimension of $H^0(E \times E, \mathcal{M}_{m,n})$ and the Euler characteristic of Corollary 17.

For $(m, n) = (2, 2)$, the dimension of $H^0(E \times E, \mathcal{M})$ is determined by Theorem 10 and Theorem 21, and for all higher bidegrees the sheaf $\mathcal{M}_{m,n}$ is ample and $\chi(E \times E, \mathcal{M}_{m,n})$ equals $\dim_k(H^0(E \times E, \mathcal{M}_{m,n}))$ by Theorem 16. \square

These dimension formulas will be generalized in Section 4, after the introduction of the concept of an addition law projection.

3.3 Dimensions of sections of the ideal sheaf

When E is embedded as a cubic curve in \mathbb{P}^2 , the defining ideal sheaf \mathcal{I}_E of E has no sections of degree 2, which is to say that $\dim_k(\Gamma(\mathbb{P}^2, \mathcal{I}_E(2))) = 0$. However, a degree 4 or higher divisor always includes quadratic defining relations. This introduces an ambiguity in the representation of an addition law by polynomials. In what follows, when E is not contained in a hyperplane of \mathbb{P}^r , the ideal sheaf contains no linear relations, and the degree d equals $r + 1$, since a projective normal embedding is given by a complete linear system.

Lemma 23 *Let E be an elliptic curve and $\iota : E \rightarrow \mathbb{P}^r$ be a projectively normal embedding of degree d . Then for the ideal sheaf \mathcal{I}_E , we have*

$$\dim_k(\Gamma(\mathbb{P}^r, \mathcal{I}_E(n))) = \binom{n+r}{r} - nd.$$

Proof Let $\mathcal{L} = \mathcal{O}_E(1)$ and note that $\Gamma(\mathbb{P}^r, \mathcal{O}(n)) \rightarrow \Gamma(E, \mathcal{L}^n)$ is surjective by hypothesis. Thus the dimension is determined by the number of monomials of degree n in $r + 1$ variables minus the dimension of the space $\Gamma(E, \mathcal{L}^n)$. This latter space has dimension nd by Riemann-Roch, from which the result follows. \square

The polynomial representatives for the coordinates of an addition law of bidegree (m, n) are well defined only up to elements of

$$I_{m,n} = \Gamma(\mathbb{P}^r, \mathcal{I}_E(m)) \otimes \Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(n)) + \Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m)) \otimes \Gamma(\mathbb{P}^r, \mathcal{I}_E(n)).$$

Since, for $d \geq 4$, the dimension of $\Gamma(\mathbb{P}^r, \mathcal{I}_E(2))$ is nonzero, the addition laws for any nonplanar model have nonunique representation by polynomials. We make this more precise in the following corollary.

Corollary 24 *An addition law of bidegree (m, n) is represented by a coset of a vector space of polynomials whose dimension is*

$$(r+1) \left(\binom{m+r}{r} \binom{n+r}{r} - d^2 mn \right).$$

Proof The dimension of the vector space $I_{m,n}$ equals

$$\binom{m+r}{r} \binom{n+r}{r} - d^2 mn,$$

determined by Lemma 23 and Möbius inversion with respect to the common vector subspace $\Gamma(\mathbb{P}^r, \mathcal{I}_E(m)) \otimes \Gamma(\mathbb{P}^r, \mathcal{I}_E(n))$. Since each of the $r + 1$ polynomials representing the addition law coordinates is a coset of the vector space $I_{m,n}$ we obtain the cofactor $r + 1$. \square

4 Addition law projections

We introduce the notion of an addition law projection first in order to define the concept of an affine addition law given by rational maps, expressed in terms of morphisms $E \times E \mapsto \mathbb{P}^1$ which factor through μ . In addition we are able to consider generalizations of addition laws which take the form $E_1 \times E_1 \rightarrow E_2$, where E_1 and E_2 are different embeddings, defined by divisors D_1 and D_2 .

4.1 Definition of an addition law projection

Let E be projectively normal in \mathbb{P}^r with $\mathcal{L} = \mathcal{O}_E(1)$, let $\varphi : E \rightarrow C \subset \mathbb{P}^s$ be a morphism, and set $\mathcal{L}_\varphi = \varphi^* \mathcal{O}_C(1)$. We assume that $\mathcal{L} \cong \mathcal{L}(D)$ and $\mathcal{L}_\varphi \cong \mathcal{L}(D_\varphi)$. We now define the space of *addition law projections* of bidegree (m, n) with respect to the composition $\varphi \circ \mu$ to be the set of $(s + 1)$ -tuples $\mathfrak{s} = (p_0, \dots, p_s)$ with

$$p_j \in \Gamma(E \times E, \pi_1^* \mathcal{L}^m \otimes \pi_2^* \mathcal{L}^n),$$

determining $\varphi \circ \mu$ on an open subvariety of $E \times E$. As above, we interpret an addition law projection \mathfrak{s} as an element of $\text{Hom}(\mu^* \mathcal{L}_\varphi, \pi_1^* \mathcal{L}^m \otimes \pi_2^* \mathcal{L}^n)$, isomorphic to

$$\Gamma(E \times E, \mu^* \mathcal{L}_\varphi^{-1} \otimes \pi_1^* \mathcal{L}^m \otimes \pi_2^* \mathcal{L}^n).$$

The principal interest is when, up to isomorphism, $D > D_\varphi > 0$, and φ is either an isomorphism or a projection to \mathbb{P}^1 . In such a case, the morphism φ has a linear representation and an addition law for μ restricts to an addition law projection for $\varphi \circ \mu$. On the other hand, the space of addition laws projections is in general larger and may be nonzero for bidegrees less than $(2, 2)$.

4.2 Dimensions of spaces of addition law projections

We are now in a position to determine the dimensions of the spaces of addition law projections. Let E be a projectively normal curve in \mathbb{P}^r with $\mathcal{L} = \mathcal{O}_E(1) \cong \mathcal{L}(D)$ and φ a nonconstant morphism to a curve C in \mathbb{P}^s such that

$$\mathcal{L}_\varphi := \varphi^* \mathcal{O}_C(1) \cong \mathcal{L}(D_\varphi)$$

and define

$$\mathcal{M}_{\varphi, m, n} = \mu^* \mathcal{L}_\varphi^{-1} \otimes \pi_1^* \mathcal{L}^m \otimes \pi_2^* \mathcal{L}^n.$$

We assume D and D_φ are effective and write $d = \deg(D)$ and $d_\varphi = \deg(D_\varphi)$. With this notation, we obtain the following refinement of Corollary 17, as a consequence of Lemma 15 and Theorem 16.

Corollary 25 $\chi(\mathcal{M}_{\varphi,m,n}) = d(dmn - d_{\varphi}(m+n)).$

When $d = 2d_{\varphi}$ the critical bidegree is $(1, 1)$, for which the Euler-Poincaré characteristic is zero, and when $d \geq 2d_{\varphi}$, the minimal bidegree of any addition law projection is $(1, 1)$, so we write simply \mathcal{M}_{φ} for the sheaf $\mathcal{M}_{\varphi,1,1}$. We can now state a generalization of Theorem 10.

Theorem 26 *Let $\iota : E \rightarrow \mathbb{P}^r$ be a projectively normal embedding of an elliptic curve, with respect to a symmetric sheaf $\mathcal{L} \cong \mathcal{L}(D)$, and let $\varphi : E \rightarrow \mathbb{P}^s$ be a nonconstant map, with respect to a symmetric sheaf $\mathcal{L}_{\varphi} \cong \mathcal{L}(D_{\varphi})$. If both \mathcal{L} and \mathcal{L}_{φ} are symmetric and $d = 2d_{\varphi}$, then the space of global sections of \mathcal{M}_{φ} is isomorphic to that of $\mathcal{L} \otimes \mathcal{L}_{\varphi}^{-1}$. Moreover, the exceptional divisor of an addition law projection of bidegree $(1, 1)$ associated to a section in $\Gamma(E \times E, \mathcal{M}_{\varphi})$ is of the form $\sum_{i=1}^{d_{\varphi}} \Delta_{P_i}$ where $D - D_{\varphi} \sim \sum_{i=1}^{d_{\varphi}} (P_i)$.*

Proof Up to equivalence of D and D_{φ} , we may assume that D , D_{φ} , and D_{ψ} are symmetric effective divisors, hence with support in $E[2]$, such that $D = D_{\varphi} + D_{\psi}$, and denote $\mathcal{L}(D_{\psi})$ by \mathcal{L}_{ψ} . By hypothesis $d = 2 \deg(D_{\psi}) = 2d_{\varphi}$. Linear extension of Lemma 8 then gives

$$\delta^* D_{\psi} + \mu^* D_{\varphi} \sim \pi_1^* D + \pi_2^* D,$$

and hence

$$\delta^* \mathcal{L}_{\psi} \otimes \mu^* \mathcal{L}_{\varphi} \cong \pi_1^* \mathcal{L} \otimes \pi_2^* \mathcal{L},$$

from which $\delta^* \mathcal{L}_{\psi} \cong \mathcal{M}$. The isomorphism of global sections and structure of the exceptional divisors follows as in Theorem 10. \square

Corollary 27 *Let \mathcal{L} , \mathcal{L}_{φ} , and $\mathcal{M}_{\varphi,m,n}$ be as above, with $d = 2d_{\varphi}$. Then for $(m, n) = (1, 1)$,*

$$\dim_k(H^0(E \times E, \mathcal{M}_{\varphi})) = \dim_k(H^1(E \times E, \mathcal{M}_{\varphi})) = d_{\varphi},$$

and for $(m, n) > (1, 1)$,

$$\dim_k(H^0(E \times E, \mathcal{M}_{\varphi,m,n})) = d_{\varphi}^2((2m-1)(2n-1)-1).$$

Proof For $(m, n) = (1, 1)$ the dimension follows from the isomorphism of Theorem 26. When $(m, n) > (1, 1)$, the sheaf \mathcal{M} is effective and $\chi(E \times E, \mathcal{M})$ positive, so the equality follows from Theorem 16 and Corollary 25. \square

Remark. As a consequence of Corollary 25, the only possible critical cases, for which $\chi(E \times E, \mathcal{M}_{\varphi,m,n}) = 0$, are those in the table below, given with the value of $h^0 = \dim_k(\Gamma(E \times E, \mathcal{M}_{\varphi,m,n}))$, if nonzero.

d	d_{φ}	(m, n)	h^0
$s(t+1)$	st	$(1, t), (t, 1)$	s
$2d_{\varphi}$	d_{φ}	$(1, 1)$	d_{φ}
d_{φ}	d_{φ}	$(2, 2)$	d_{φ}

The latter two cases are explained by Theorem 10 and Theorem 26. By Theorem 20, the exceptional divisor is numerically equivalent to a divisor of the form $n\Gamma_{(a,b)}$. For $d = 2d_\varphi$ and $d = d_\varphi$, this divisor is $d_\varphi\Delta$, but for $(d, d_\varphi) = (s(t+1), st)$, the exceptional divisor is numerically equivalent to $s\Gamma_{(1,t)}$ or $s\Gamma_{(t,1)}$. Theorem 34 of Section 8 gives an example of an elliptic curve with one-dimensional spaces of addition laws projections of bidegrees $(1, 2)$ and $(2, 1)$ for $(d, d_\varphi) = (3, 2)$.

5 Affine models and projective normal closure

A nonsingular projective curve is uniquely determined, up to unique isomorphism, by an affine model C [10, Chapter I, Corollary 6.12]. As a consequence, it is standard to specify a curve by an affine model which determines it. On the other hand, the definition of addition laws in terms of a given affine model depends on the projections to \mathbb{P}^1 given by the coordinate functions. In this section we introduce the notion of a projective normal closure of a nonsingular affine model C . This provides a canonical nonsingular projective model in which C embeds, in terms of which we define affine addition laws. In Section 6 we apply this definition in order to determine dimension formulas for affine addition laws.

5.1 Projective normal closure

Let C/k be a nonsingular affine curve in \mathbb{A}^s , with coordinate functions x_1, \dots, x_s and X its associated nonsingular projective curve. We define the *divisor at infinity* of C to be the effective divisor $D = \sup(\{\text{div}_\infty(x_i)\})$, on X , where $\text{div}_\infty(x)$ is the polar divisor of x .

Let $\{x_0, x_1, \dots, x_r\}$ be a generator set for $\Gamma(X, \mathcal{L}(D))$, where we assume $x_0 = 1$, and x_1, \dots, x_s are the coordinate functions on C . Since C is nonsingular, its coordinate ring is integrally closed, and by the definition of D , we have

$$k[x_1, \dots, x_s] = k[x_1, \dots, x_r].$$

A *projectively normal closure* of C is a model for X in \mathbb{P}^r , determined by the morphism

$$P \longmapsto (x_0(P) : x_1(P) : \dots : x_r(P)),$$

which identifies C as the open affine of X given by $X_0 = 1$. Any two projectively normal closures are isomorphic via a linear isomorphism determined by the choice of generator set extending x_0, \dots, x_s .

Jacobi model. The Jacobi quartic refers to the nonsingular affine curve

$$y^2 = x^4 + 2ax^2 + 1,$$

with base point $O = (0, 1)$, and whose standard projective closure in \mathbb{P}^2 is singular. The divisor at infinity is $D = 2(\infty_1) + 2(\infty_2)$, and the Riemann-Roch space $\Gamma(E, \mathcal{L}(D))$ is spanned by $\{1, x, y, x^2\}$. Thus the projective normal

closure is the curve C in \mathbb{P}^3 given by the embedding $(x, y) \mapsto (1 : x : y : x^2)$, with defining equations

$$X_2^2 = X_0^2 + 2aX_0X_3 + X_3^2, \quad X_0X_3 = X_1^2,$$

and identity $(1 : 0 : 1 : 0)$.

The Jacobi quartic has full rational 2-torsion, which accounts for the symmetries. In Section 8 we describe a canonical Jacobi model, diagonalized with respect to the 2-torsion subgroup, and which contains this family as a subfamily up to linearly isomorphism.

Edwards model. In 2007, Edwards [9] introduced a remarkable new affine model for elliptic curves

$$x^2 + y^2 = c^2(1 + dx^2y^2).$$

The parameter d , equal to 1 in Edwards' model, was introduced by Bernstein and Lange [1], to obtain an k -complete addition law for nonsquare values of d (and moreover the parameter c may be subsumed into d as a square factor). Subsequently, Bernstein et al. [2] introduced twisted Edwards curves

$$ax^2 + y^2 = 1 + dx^2y^2.$$

The divisor at infinity is $D = \operatorname{div}(x)_\infty + \operatorname{div}(y)_\infty$, since the poles of x and y are disjoint. A basis for the Riemann-Roch space of D is then $\{1, x, y, xy\}$, and the projective normal closure in \mathbb{P}^3 is

$$X_0^2 + dX_3^2 = aX_1^2 + X_2^2, \quad X_0X_3 = X_1X_2,$$

with embedding $(x, y) \mapsto (1 : x : y : xy)$. This embedding in \mathbb{P}^3 appears in Hisil et al. [11], under the name extended Edwards coordinates.

5.2 Arithmetically complete affine models

The notion of completeness of addition laws is sometimes coupled with an independent condition on a particular affine model. By definition an abelian variety is a complete group variety – completeness is a geometric notion which is stable under base extension. We define an affine curve C to be k -complete or *arithmetically complete* if $C(k) = X(k)$ for any projective nonsingular X containing C . For an elliptic curve, this ensures that the rational points of the affine model form a group. Over a sufficiently large base field, one can find a suitable line which misses all rational points and pass to a k -complete affine model by a projective change of variables.

In the above example of a projective normal closure for the Jacobi quartic, the affine patch $X_2 = 1$:

$$1 = u^2 + 2auw + w^2, \quad uw = v^2,$$

is k -complete if $x^2 + 2ax + 1$ is irreducible. The affine patch $X_3 = 1$ of the projective normal closure of the twisted Edwards model recovers the standard affine representation, which is k -complete when d is a nonsquare. An additional feature of the k -complete models for twisted Edwards curves [2] or twisted Hessian curves [4] is that the line at infinity is an eigenvector for a torsion subgroup, which acts linearly on the affine curve.

6 Affine addition laws

Suppose that C is a nonsingular affine curve in \mathbb{A}^s and let E be a projective normal closure of C in \mathbb{P}^r . If x_1, \dots, x_s are the coordinate functions on C , then we denote by x_i also the projections $E \rightarrow \mathbb{P}^1$ extending $x_i : C \rightarrow \mathbb{A}^1$. Let $k[C] = k[x_1, \dots, x_s]$ be the coordinate ring of C , recalling that since C is nonsingular, $k[x_1, \dots, x_s] = k[x_1, \dots, x_r] = \Gamma(C, \mathcal{O}_E)$, where $x_i = X_i/X_0$. We write

$$k[C] \otimes_k k[C] = k[x_1, \dots, x_r, y_1, \dots, y_r]$$

where we identify x_i with $x_i \otimes 1$ and write y_i for $1 \otimes x_i$, and similarly identify X_i with

$$X_i \otimes 1 \in \Gamma(E \times E, \pi_1^* \mathcal{O}_E(1) \otimes \pi_2^* \mathcal{O}_E(0)),$$

and write Y_i for

$$1 \otimes X_i \in \Gamma(E \times E, \pi_1^* \mathcal{O}_E(0) \otimes \pi_2^* \mathcal{O}_E(1)).$$

An affine addition law for C is an s -tuple of pairs (f_i, g_i) in $(k[C] \otimes_k k[C])^2$ such that

$$\mu^*(x_i) = \frac{f_i}{g_i} \in k(E \times E).$$

We refer to (f_i, g_i) as an *affine addition law projection* for x_i . We define the *bidegree* of an addition law $\mathfrak{s}_i = (f_i, g_i)$ to be the smallest m_i and n_i such that \mathfrak{s}_i is the restriction of an addition law projection of bidegree (m_i, n_i) , and the bidegree of $\mathfrak{s} = (\mathfrak{s}_1, \dots, \mathfrak{s}_s)$ to be $(m, n) = (\max_i(\{m_i\}), \max_i(\{n_i\}))$. We note that the bidegree of an addition law is determined by the minimal degree polynomial expression in $\{x_1, \dots, x_r, y_1, \dots, y_r\}$ for f_i and g_i , rather than as a polynomial in the coordinate functions on $\{x_1, \dots, x_s, y_1, \dots, y_s\}$.

Recall that the product partial order is defined by $(k, l) \leq (m, n)$ if and only if $k \leq m$ and $l \leq n$. Clearly an addition law projection of bidegree (k, l) is also the restriction of an addition law projection of bidegree (m, n) when $(k, l) \leq (m, n)$, since the restriction map associated to $C \rightarrow E$ is the homomorphism which forgets the grading:

$$k[E] \cong \bigoplus_{n=0}^{\infty} \Gamma(E, nD) \longrightarrow k[C] = \Gamma(C, \mathcal{O}_E) = \bigcup_{n=0}^{\infty} \Gamma(E, nD).$$

For convenience, we say the space of addition laws (or addition law projections) of bidegree (m, n) , to refer to the vector space of all addition laws (or addition law projections) of any bidegree $(k, l) \leq (m, n)$.

Hereafter we express an affine addition law projection (f_i, g_i) as a fraction f_i/g_i and similarly write

$$\mathfrak{s} = \left(\frac{f_1}{g_1}, \frac{f_2}{g_2}, \dots, \frac{f_s}{g_s} \right),$$

for an affine addition law. We note that in this context f_i/g_i should not be confused with the equivalence class $z_i = \mu^*(x_i)$ in $k(E \times E)$, and that in this notation the vector space structure is written:

$$a \frac{f_i}{g_i} + b \frac{f'_i}{g'_i} = \frac{af_i + bf'_i}{ag_i + bg'_i}.$$

Since $f_i = g_i z_i$ and $f'_i = g'_i z_i$, the equivalence class in $k(E \times E)$ remains the same:

$$a \frac{f_i}{g_i} + b \frac{f'_i}{g'_i} = a \frac{g_i z_i}{g_i} + b \frac{g'_i z_i}{g'_i} = \frac{(ag_i + bg'_i) z_i}{ag_i + bg'_i}.$$

Theorem 28 *The affine addition laws for C in \mathbb{A}^s of bidegree (m, n) form a vector space isomorphic to the direct sum of the spaces of addition law projections for the coordinate functions x_1, \dots, x_s of bidegree (m, n) .*

Proof Every polynomial form p_i in $\Gamma(E \times E, \pi_1^* \mathcal{O}_E(m) \otimes \pi_2^* \mathcal{O}_E(n))$ determines a unique function $f_i = p_i/X_0^n Y_0^n$ in

$$k[C] \otimes k[C] = \Gamma(C, \mathcal{O}_E) \otimes \Gamma(C, \mathcal{O}_E)$$

and injectivity of $p_i \mapsto f_i$ follows from injectivity of $\Gamma(E, \mathcal{O}_E(m)) \rightarrow k[C]$. \square

7 Torsion module structure

Let E/k be an elliptic curve with finite torsion subgroup $G \subset E(k)$. A divisor D is said to be G -invariant if $\tau_P^* D = D$ for all P in G , where $\tau_P : E \rightarrow E$ is the translation-by- P morphism. We hereafter assume that E/k is equipped with a projectively normal embedding in \mathbb{P}^r by $\mathcal{L} = \mathcal{L}(D)$, where D is an effective G -invariant divisor.

Lemma 29 *Let $\iota : E \rightarrow \mathbb{P}^r$ be a projectively normal embedding of E , with respect to \mathcal{L} . Let G be a finite torsion subgroup, and suppose that $\mathcal{L} = \mathcal{L}(D)$ where D is an effective G -invariant divisor. Then G acts on E by projective linear transformations of \mathbb{P}^r .*

Proof Since D is G -invariant, the space $\Gamma(E, \mathcal{L})$ has a k -linear representation by G . Since we have a surjective homomorphism $\Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(1)) \rightarrow \Gamma(E, \mathcal{L})$, every linear automorphism of $\Gamma(E, \mathcal{L})$ lifts to an automorphism of $\Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(1))$, hence to a projective linear transformation of \mathbb{P}^r . \square

From the action of τ_P^* on $\Gamma(E, \mathcal{L})$, and lifting to $\Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(1))$, we identify τ_P with a linear polynomial map in $k[X_0, \dots, X_r]^{r+1}$. Let G_2 be the kernel of

the homomorphism $G \times G \times G \rightarrow G$ defined by $(R, S, T) \mapsto R + S + T$, and let G_1 be the subgroup of G_2 with $T = 0$. We define the action of G_2 (hence of G_1) on the space of addition laws of bidegree (m, n) by $(R, S, T) \cdot \mathfrak{s} = \tau_T \circ \mathfrak{s} \circ (\tau_R \times \tau_S)$, so that

$$(R, S, T) \cdot \mathfrak{s}(P, Q) = \mathfrak{s}(P + R, Q + S) + T.$$

Clearly G_1 and G_2 are isomorphic to G and $G \times G$, respectively, with isomorphisms given by $R \mapsto (R, -R, O)$ and $(R, S) \mapsto (R, S, -R - S)$.

Lemma 30 *The group G_2 acts linearly on the addition laws of bidegree (m, n) .*

Proof The image $(R, S, T) \cdot \mathfrak{s}$ is the composition of polynomials of bidegree (m, n) with linear polynomial maps, which, by the hypothesis that $R + S + T = O$, determines another addition law. \square

Lemma 31 *The group G_2 acts linearly on the set of divisors of addition laws for E . In particular the action on the components of addition laws of bidegree $(2, 2)$ is given by $(R, S, T)^* \Delta_P = \Delta_{P-R+S}$.*

Proof The action on divisors is $\text{div}((R, S, T) \cdot \mathfrak{s}) = (\tau_R \times \tau_S)^* \text{div}(\mathfrak{s})$, and the action on Δ_P follows from

$$(\tau_R \times \tau_S)^* \Delta_P = \Delta + (P - R, -S) = \Delta + (P - R + S, O) = \Delta_{P-R+S}.$$

Since T determines a linear automorphism of the polynomials of \mathfrak{s} , it has no bearing on the divisor which they cut out. \square

Theorem 32 *An addition law \mathfrak{s} is an eigenvector for an element (R, S, T) of G_2 if and only if the exceptional divisor of \mathfrak{s} is fixed by (R, S, T) .*

The abstract vector spaces of addition laws, as well as the G_2 -module structure are independent of the choice of bases for $\Gamma(E, \mathcal{L})$ as well as $\Gamma(E \times E, \mathcal{M})$. However, the simplicity of the addition laws (as measured, for example, by their sparseness as polynomials) on Edwards and Hessian models, is entirely dependent on the choice of the sections in $\Gamma(E, \mathcal{L})$ and the corresponding coordinate functions of the projective embedding, and of the addition laws. This study grew out of the observation that the simplest addition laws arise from the bases which arise either as eigenspaces of G_1 or which have a permutation representation with respect to G_1 .

For a group G acting linearly on a space of addition laws (for which we may consider G of the form G_1 or G_2 as above), we define an addition law \mathfrak{s} to be G -complete if $\{\gamma \mathfrak{s} : \gamma \in G\}$ is a geometrically complete set of addition laws (see [4]).

8 Addition law constructions

In this section we apply the above analysis to determine and characterize the spaces of addition laws for families with rational torsion subgroups or rational

torsion points. In view of Lemma 5, we consider families with rational d -torsion subgroups for elliptic curve models of degree d .

The complete spaces of addition laws of given bidegree can be determined for any effective addition algorithm by interpolating of points $((P, Q), \mu(P, Q))$ with monomials of the correct bidegree. Such an approach was suggested by D. Bernstein and T. Lange, and a similar interpolation algorithm appears in Castyck and Vercauteren [7]. On a generic model, for which there may exist only finitely many rational points, we interpolate points in the formal neighborhood of O or the rational torsion points. Hisil et al. [12] use an analogous approach through Gröbner bases, based on an algorithm of Monagan and Pierce [19], to systematically search for rational expressions for affine addition laws. Using the automorphisms induced by torsion points, the spaces of addition laws can be reduced and distinguished eigenspaces computed directly. Algorithms for the analysis of addition laws and group actions was written in Magma [18] and Sage [23], to be made available in Echidna [14].

For known families, particularly Edwards curves, the classification in terms of eigenspaces explains the canonical nature of the distinguished prescribed addition laws reported in the literature.

8.1 Symmetric elliptic curve models of degree 3

Hessian model. The Hessian model $H_d/k : X^3 + Y^3 + Z^3 = dXYZ$ is well known as a universal model (over $k(X(3))$) for elliptic curves with full torsion subgroup. In Bernstein, Kohel, and Lange [4], the twisted Hessian curves $H_{(a,d)}/k$:

$$aX^3 + Y^3 + Z^3 = dXYZ,$$

are introduced (a descent of scalars to $k(X_0(3))$), and their addition laws and completeness properties are studied. In characteristic different from 3, in terms of the order 3 subgroup G defined by $X = 0$, we can characterize the addition laws terms of their G_1 -module structure [4].

Theorem 33 *The space of addition laws of bidegree $(2, 2)$ for the twisted Hessian curve is spanned by the three addition laws:*

$$\begin{aligned} \mathfrak{s}_0 &= (X_1^2 Y_2 Z_2 - Y_1 Z_1 X_2^2, Z_1^2 X_2 Y_2 - X_1 Y_1 Z_2^2, Y_1^2 X_2 Z_2 - X_1 Z_1 Y_2^2), \\ \mathfrak{s}_1 &= (X_1 Y_1 Y_2^2 - Z_1^2 X_2 Z_2, a X_1 Z_1 X_2^2 - Y_1^2 Y_2 Z_2, Y_1 Z_1 Z_2^2 - a X_1^2 X_2 Y_2), \\ \mathfrak{s}_2 &= (X_1 Z_1 Z_2^2 - Y_1^2 X_2 Y_2, Y_1 Z_1 Y_2^2 - a X_1^2 X_2 Z_2, a X_1 Y_1 X_2^2 - Z_1^2 Y_2 Z_2). \end{aligned}$$

Each \mathfrak{s}_i is an eigenvector for the action of G_1 .

Remark. The addition laws are also simultaneous eigenvectors for the full subgroup G_2 . Over an extension in which a is a cube root, the curve attains an independent 3-torsion point, which acts by scaled coordinate permutation. Consequently the addition laws are cyclically permuted under this action. This action on the addition law (4.21i) of Chudnovsky and Chudnovsky [8], in retrospect, is sufficient to produce the above basis.

Similarly an explicit computation yields the following addition law projections of bidegrees $(1, 2)$ and $(2, 1)$.

Theorem 34 *The twisted Hessian curve admits degree 2 coordinate projections*

$$(X : X - T), \quad (Y : Y - T), \quad \text{and} \quad (Z : Z - T),$$

where $T = X + Y + Z$, for which there exist addition laws of bidegree $(1, 2)$:

$$\begin{aligned} & (X_1 Y_2 Z_2 + Y_1 X_2 Y_2 + Z_1 X_2 Z_2 : X_1 X_2^2 + Y_1 Z_2^2 + Z_1 Y_2^2), \\ & (X_1 X_2 Z_2 + Y_1 Y_2 Z_2 + Z_1 X_2 Y_2 : X_1 Y_2^2 + Y_1 X_2^2 + Z_1 Z_2^2), \\ & (X_1 X_2 Y_2 + Y_1 X_2 Z_2 + Z_1 Y_2 Z_2 : X_1 Z_2^2 + Z_1 X_2^2 + Y_1 Y_2^2), \end{aligned}$$

and of bidegree $(2, 1)$:

$$\begin{aligned} & (Y_1 Z_1 X_2 + X_1 Y_1 Y_2 + X_1 Z_1 Z_2 : X_1^2 X_2 + Z_1^2 Y_2 + Y_1^2 Z_2), \\ & (X_1 Z_1 X_2 + Y_1 Z_1 Y_2 + X_1 Y_1 Z_2 : Y_1^2 X_2 + X_1^2 Y_2 + Z_1^2 Z_2), \\ & (X_1 Y_1 X_2 + X_1 Z_1 Y_2 + Y_1 Z_1 Z_2 : Z_1^2 X_2 + Y_1^2 Y_2 + X_1^2 Z_2). \end{aligned}$$

Each addition laws projection spans the unique one-dimensional space of its bidegree.

Remark. This provides an example of an addition law projection of the critical bidegree in Corollary 25, at which the Euler-Poincaré characteristic is zero (see the remark following Corollary 27). Note that the projections $(X : X - T)$ and $(X : T)$ are linearly equivalent, but the former yields a simpler expression.

8.2 Symmetric elliptic curves of degree 4

Next we consider degree 4 models of elliptic curves, with parametrized 2-torsion and 4-torsion subgroups. In order to be diagonalized with respect to the torsion subgroup, we assume that the base field is not of characteristic 2.

Jacobi model. Let $J_{(a,b)}$ be the elliptic curve over a field of characteristic different from 2, given by the quadric intersections in \mathbb{P}^3 :

$$\begin{aligned} aX_0^2 + X_1^2 &= X_2^2, \\ bX_0^2 + X_2^2 &= X_3^2, \\ cX_0^2 + X_3^2 &= X_1^2, \end{aligned}$$

where $a + b + c = 0$, with identity $O = (0 : 1 : 1 : 1)$ and 2-torsion points

$$T_1 = (0 : -1 : 1 : 1), \quad T_2 = (0 : 1 : -1 : 1), \quad T_3 = (0 : 1 : 1 : -1).$$

The embedding in \mathbb{P}^3 is given by a complete linear system associated to any divisor equivalent to the sum of the 2-torsion points, which in canonical form of Lemma 2 is $4(O)$.

Theorem 35 *Let E/k be an elliptic curve with projective normal embedding in \mathbb{P}^3 such that $\mathcal{O}_E(1) \cong \mathcal{L}(4(O))$. If $E(k)[2]$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, then there exists (a, b) in k^2 such that E is linearly isomorphic to $J_{(a,b)}$.*

Proof The j -invariant of the family $J_{(a,b)}$ determines an S_3 cover j -line by $(a : b)$ in \mathbb{P}^1 , ramified over $j = 0$ and $j = 12^3$, and by construction $(a : b)$ represents a point on the modular curve $X(2)$. Thus for j different from 0 and 12^3 , it follows that $J_{(a,b)}$ encodes a representative elliptic curve with full 2-torsion, and its quadratic twists, associated to each point on $X(2)$.

For the exceptional values $j = 0$ and $j = 12^3$, we first suppose that $\text{char}(k) \neq 3$, so that $0 \neq 12^3$ (since $\text{char}(k) \neq 2$ by hypothesis). An elliptic curve with $j = 0$ or $j = 12^3$ is then isomorphic to $y^2 = x^3 - s^3$ or $y^2 = x^3 - s^2x$, respectively. In the former case, by hypothesis on the 2-torsion, there exists ω in k such that $\omega^2 = -\omega - 1$, and cubic and quartic twists do not have full 2-torsion. Jacobi models for these curves are, respectively,

$$\begin{aligned} (2\omega + 1)sX_0^2 + X_1^2 &= X_2^2, & 2sX_0^2 + X_1^2 &= X_2^2, \\ w(2\omega + 1)sX_0^2 + X_2^2 &= X_3^2, & -sX_0^2 + X_2^2 &= X_3^2, \\ w^2(2\omega + 1)sX_0^2 + X_3^2 &= X_1^2, & -sX_0^2 + X_3^2 &= X_1^2. \end{aligned}$$

In characteristic 3, the latter model describes all twists over k of the unique supersingular elliptic curve over \mathbb{F}_3 with $j = 12^3 = 0$ and full 2-torsion. The linearity of the isomorphisms follows from Lemma 3. \square

Example. Chudnovsky and Chudnovsky [8, Section 4] define a Jacobi quadric intersection

$$\begin{aligned} x^2 + y^2 &= 1, \\ \lambda^2 x^2 + z^2 &= 1, \end{aligned}$$

which is an affine model for a curve in this family for $(a, b, c) = (1, -\lambda^2, \lambda^2 - 1)$, with the embedding

$$(x, y, z) \mapsto (x : y : 1 : z).$$

This gives an example of a nonsingular affine model, which is k -complete over any field k in which -1 is not a square.

Similarly, the projective normal closure of the Jacobi quartic (see Section 5):

$$X_2^2 = X_0^2 + 2aX_0X_3 + X_3^2, \quad X_0X_3 = X_1^2,$$

is isomorphic to the Jacobi model with $(a, b, c) = (-2(a+1), 4, 2(a-1))$, by the transformation $(X_0 : X_1 : X_2 : X_3) \mapsto (X_1 : X_2 : X_0 - X_3 : X_0 + X_3)$.

Theorem 36 *The space of addition laws of bidegree $(2, 2)$ for $J_{(a,b)}$ is spanned by $\{\mathfrak{s}_i : 0 \leq i \leq 3\}$, where*

$$\begin{aligned} \mathfrak{s}_0 &= (X_0^2Y_1^2 - X_1^2Y_0^2, & \mathfrak{s}_1 &= (X_0X_2Y_1Y_3 + X_1X_3Y_0Y_2, \\ & X_0X_1Y_2Y_3 - X_2X_3Y_0Y_1, & & -aX_0X_3Y_0Y_3 + X_1X_2Y_1Y_2, \\ & X_0X_2Y_1Y_3 - X_1X_3Y_0Y_2, & & abX_0^2Y_0^2 + X_2^2Y_2^2, \\ & X_0X_3Y_1Y_2 - X_1X_2Y_0Y_3), & & bX_0X_1Y_0Y_1 + X_2X_3Y_2Y_3), \\ \mathfrak{s}_2 &= (X_0X_1Y_2Y_3 + X_2X_3Y_0Y_1, & \mathfrak{s}_3 &= (a(X_0X_3Y_1Y_2 + X_1X_2Y_0Y_3), \\ & acX_0^2Y_0^2 + X_1^2Y_1^2, & & a(cX_0X_2Y_0Y_2 + X_1X_3Y_1Y_3), \\ & aX_0X_3Y_0Y_3 + X_1X_2Y_1Y_2, & & a(-bX_0X_1Y_0Y_1 + X_2X_3Y_2Y_3), \\ & -cX_0X_2Y_0Y_2 + X_1X_3Y_1Y_3), & & -bX_1^2Y_1^2 - cX_2^2Y_2^2) \end{aligned}$$

and the exceptional divisor of \mathfrak{s}_i is $\delta^*(D_i)$ where D_i is defined by $X_i = 0$.

Proof The dimension of the space of addition laws of bidegree $(2, 2)$ is four by Corollary 22. The exceptional divisors are of the form $\delta^*(D_i)$ by Theorem 10, and the divisors D_i are determined by intersecting with $J_{(a,b)} \times \{O\}$. \square

Corollary 37 *The addition laws $\mathfrak{s}_0, \mathfrak{s}_1, \mathfrak{s}_2$ and \mathfrak{s}_3 are common eigenvectors for the translations τ_{T_i} and $[-1]$.*

Proof Since each of the divisors D_i is fixed by $\tau_{T_i}^*$ and $[-1]^*$, the addition laws are immediately eigenvectors. \square

There exists a torsion point of order 4 on $J_{(a,b)}$ if and only if a pair $\{a, -c\}$, $\{-a, b\}$, or $\{-b, c\}$ consists of squares (namely the 4-torsion points lie on $X_1 = 0$, $X_2 = 0$, or $X_3 = 0$, respectively). Any such point then acts linearly on the space $\Gamma(J_{(a,b)}, \mathcal{L}(4(O)))$ by Lemma 5.

Corollary 38 *Suppose that G is a cyclic subgroup of order 4 in $J_{(a,b)}(k)$. Then any \mathfrak{s} in $\{\mathfrak{s}_0, \mathfrak{s}_1, \mathfrak{s}_2, \mathfrak{s}_3\}$ is G_2 -complete where G_2 is defined with respect to G .*

Proof The group G_2 commutes with the 2-torsion subgroup, hence induces a permutation on the set of eigenspaces spanned by the \mathfrak{s}_i . In view of Lemma 31, the group G_2 includes an element permuting two pairs of eigenspaces. Since the exceptional divisors of Theorem 36 are pairwise disjoint, any two of the s_i comprise a geometrically complete set. \square

Edwards models. Let $E_1 = E_{(a,d)}$ be the projective normal closure of the twisted Edwards model (see Section 5)

$$X_0^2 + dX_3^2 = aX_1^2 + X_2^2, \quad X_0X_3 = X_1X_2.$$

In view of the role of the projective addition laws, we define its image in $\mathbb{P}^1 \times \mathbb{P}^1$:

$$E_2 : aX^2W^2 + Y^2Z^2 = Z^2W^2 + dX^2Y^2,$$

given by

$$(X_0 : X_1 : X_2 : X_3) \mapsto ((X : Z), (Y : W)) = ((X_0 : X_1), (X_0 : X_2)),$$

which is nonsingular. It follows that the embedding in \mathbb{P}^3 is the image of the Segre embedding

$$((X : Z), (Y : W)) \longmapsto (XY : XW : ZY : ZW) = (X_0 : X_1 : X_2 : X_3).$$

Here we describe the interplay between the embedding in \mathbb{P}^3 and $\mathbb{P}^1 \times \mathbb{P}^1$, exploited in the simple addition laws of Hisil [11] for models in \mathbb{P}^3 , and interpret the addition laws and their completeness properties in terms of eigenspaces under the 4-torsion subgroup. The addition laws so determined on the curve E_2 embedded in $\mathbb{P}^1 \times \mathbb{P}^1$ are those studied by Bernstein and Lange [3], who prove their completeness properties. The above theory gives a means of explaining the canonical nature of these simple addition laws.

Suppose that c and e are square roots of a and d , respectively, in the algebraic closure of the base field of E_2 . Then $T_1 = (0 : 1 : 0 : c)$ and $T_2 = (1 : 0 : e : 0)$ are points of order 4, and the translation-by- T_1 morphism is

$$(X_0 : X_1 : X_2 : X_3) \mapsto (-X_0 : c^{-1}X_2 : -cX_1 : X_3),$$

and that for translation-by- T_2 is:

$$(X_0 : X_1 : X_2 : X_3) \mapsto (-e^{-1}X_3 : X_1 : -X_2 : eX_0).$$

We note that $2T_1 = 2T_2 = (0 : 0 : -1 : 1)$,

$$T_1 + T_2 = (-c : e : 0 : 0) \text{ and } T_1 - T_2 = (c : e : 0 : 0)$$

and $E_1[2] = \{O, 2T_i, T_1 \pm T_2\}$. Let G be the torsion subgroup $\langle T_1, T_2 \rangle$, isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. We now state the characterization of the spaces of addition laws for the group morphism $E_1 \times E_1 \rightarrow E_2$, in terms of bases of distinguished eigenvectors and their exceptional divisors. These addition laws, as well as the characterization of exceptional divisors, can be deduced from the addition laws for $E_2 \times E_2 \rightarrow E_2$ of Bernstein and Lange [3], by factoring through the Segre embedding (see note below Corollary 43).

Theorem 39 *The space of addition laws for $E_1 \times E_1 \rightarrow E_2$ of bidegree $(1, 1)$ is spanned by $\{(\mathfrak{s}_i, \mathfrak{t}_j) : 0 \leq i, j \leq 1\}$, where*

$$\begin{aligned} \mathfrak{s}_0 &= (X_0Y_3 + X_3Y_0, aX_1Y_1 + X_2Y_2), \\ \mathfrak{s}_1 &= (X_1Y_2 + X_2Y_1, dX_0Y_0 + X_3Y_3), \end{aligned}$$

with respective exceptional divisors $\Delta_{T_1} + \Delta_{-T_1}$ and $\Delta_{T_2} + \Delta_{-T_2}$, and

$$\begin{aligned} \mathfrak{t}_0 &= (X_0Y_3 - X_3Y_0, X_1Y_2 - X_2Y_1), \\ \mathfrak{t}_1 &= (aX_1Y_1 - X_2Y_2, dX_0Y_0 - X_3Y_3), \end{aligned}$$

with respective exceptional divisors $\Delta_O + \Delta_{2T_i}$ and $\Delta_{T_1+T_2} + \Delta_{T_1-T_2}$.

Proof The correctness of the addition laws is verified by explicit substitution. The dimension of each of the addition law projections is 2, in accordance with Corollary 27 and the degrees of the projections of E_2 to \mathbb{P}^1 . Thus the two sets $\{\mathfrak{s}_0, \mathfrak{s}_1\}$ and $\{\mathfrak{t}_0, \mathfrak{t}_1\}$ are bases for the spaces of addition law projections. Correctness of the exceptional divisors can be verified by intersection with $E \times \{O\}$. \square

Let G_1 and G_2 be the subgroups defined in the previous section, with respect to the group $G = \langle T_1, T_2 \rangle$. The group G_1 has a well-defined action on the two spaces spanned by $\{\mathfrak{s}_0, \mathfrak{s}_1\}$ and $\{\mathfrak{t}_0, \mathfrak{t}_1\}$, while the action of G_2 only becomes well defined on the span of tuples $\{(\mathfrak{s}_i, \mathfrak{t}_j)\}$.

Corollary 40 *The sets $\{\mathfrak{s}_0, \mathfrak{s}_1\}$ and $\{\mathfrak{t}_0, \mathfrak{t}_1\}$ are stabilized by G_1 and pointwise fixed by the subgroup $\langle (2T_i, 2T_i, O) \rangle$. Moreover each of $k\mathfrak{s}_j$ and $k\mathfrak{t}_j$ are eigenspaces for the action of G_1 . The action of G_2 stabilizes the sets of pairs $\{(k\mathfrak{s}_0, k\mathfrak{t}_0), (k\mathfrak{s}_1, k\mathfrak{t}_1)\}$ and $\{(k\mathfrak{s}_0, k\mathfrak{t}_1), (k\mathfrak{s}_1, k\mathfrak{t}_0)\}$, and acts transitively on their product.*

Proof By Theorem 32, the eigenvectors are characterized by the action on the exceptional divisors. By Lemma 7 and the form of the exceptional divisors in Theorem 39, we see that the exceptional divisors are stabilized by $(T_i, -T_i, O)$ and hence $\mathfrak{s}_0, \mathfrak{s}_1, \mathfrak{t}_0$ and \mathfrak{t}_1 are eigenvectors. By explicit substitution we find eigenvalues $(-1, 1, -1, 1)$ for T_1 and eigenvalues $(1, -1, -1, 1)$ for T_2 . Hence each of the spaces spanned by $\{\mathfrak{s}_0, \mathfrak{s}_1\}$ and $\{\mathfrak{t}_0, \mathfrak{t}_1\}$ decomposes into one-dimensional eigenspaces. The action on eigenspace pairs follows similarly from the action on exceptional divisors. \square

Theorem 41 *The addition law projection $\mathfrak{s}_0, \mathfrak{s}_1$, or \mathfrak{t}_1 is k -complete if and only if a, d , or ad is a nonsquare, respectively. In particular, over a finite field, either zero or two of $\mathfrak{s}_0, \mathfrak{s}_1$ and \mathfrak{t}_1 are k -complete.*

Proof The sets $\{T_1, -T_1\}$, $\{T_2, -T_2\}$ and $\{T_1+T_2, T_1-T_2\}$ are Galois orbits of non- k -rational points when a, d , or ad is a nonsquare, respectively, in which case the respective divisor $\Delta_{T_1} + \Delta_{-T_1}$, $\Delta_{T_2} + \Delta_{-T_2}$ or $\Delta_{T_1+T_2} + \Delta_{T_1-T_2}$, is irreducible over k and hence has no rational point. Over a finite field, either zero or two of a, d , and ad are nonsquares. \square Let $\varphi : E_2 \times E_2 \rightarrow E_1$ be the restriction of the Segre embedding $\mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^3$, and identify φ with the polynomial map

$$((X, Z), (Y, W)) \mapsto (XY, XW, ZY, ZW).$$

As a consequence of the above theorem, the four-dimensional space of addition laws for E_1 is obtained in factored form as the pairwise combination of these pairs of addition laws, under the Segre embedding in \mathbb{P}^3 .

Corollary 42 *The space of addition laws of bidegree $(2, 2)$ for*

$$\mu : E_1 \times E_1 \longrightarrow E_1$$

is spanned by $\{\varphi(\mathfrak{s}_i, \mathfrak{t}_j) : 0 \leq i, j \leq 1\}$.

Similarly, we obtain a factored form $E_2 \times E_2 \rightarrow E_1 \times E_1 \rightarrow E_2$ for the addition laws on E_2 .

Corollary 43 *The space of addition laws of multidegree $((1, 1), (1, 1))$ for*

$$\mu : E_2 \times E_2 \longrightarrow E_2$$

is spanned by $\{(\mathfrak{s}_i \circ \varphi \times \varphi, \mathfrak{t}_j \circ \varphi \times \varphi) : 0 \leq i, j \leq 1\}$.

In expanded form Corollary 42 gives the addition laws:

$$\begin{aligned} \varphi(\mathfrak{s}_0, \mathfrak{t}_0) &= ((X_0Y_3 + X_3Y_0)(X_0Y_3 - X_3Y_0), (X_0Y_3 + X_3Y_0)(X_1Y_2 - Y_1X_2), \\ &\quad (aX_1Y_1 + X_2Y_2)(X_0Y_3 - X_3Y_0), (aX_1Y_1 + X_2Y_2)(X_1Y_2 - Y_1X_2)), \\ \varphi(\mathfrak{s}_0, \mathfrak{t}_1) &= ((X_0Y_3 + X_3Y_0)(aX_1Y_1 - X_2Y_2), (X_0Y_3 + X_3Y_0)(aX_1Y_1 - X_2Y_2), \\ &\quad (aX_1Y_1 + X_2Y_2)(dX_0Y_0 - X_3Y_3), (aX_1Y_1 + X_2Y_2)(dX_0Y_0 - X_3Y_3)), \\ \varphi(\mathfrak{s}_1, \mathfrak{t}_0) &= ((X_1Y_2 + X_2Y_1)(X_0Y_3 - X_3Y_0), (X_1Y_2 + X_2Y_1)(X_1Y_2 - Y_1X_2), \\ &\quad (dX_0Y_0 + X_3Y_3)(X_0Y_3 - X_3Y_0), (dX_0Y_0 + X_3Y_3)(X_1Y_2 - Y_1X_2)), \\ \varphi(\mathfrak{s}_1, \mathfrak{t}_1) &= ((X_1Y_2 + X_2Y_1)(aX_1Y_1 - X_2Y_2), (X_1Y_2 + X_2Y_1)(dX_0Y_0 - X_3Y_3), \\ &\quad (dX_0Y_0 + X_3Y_3)(aX_1Y_1 - X_2Y_2), (dX_0Y_0 + X_3Y_3)(dX_0Y_0 - X_3Y_3)). \end{aligned}$$

The forms $\varphi(\mathfrak{s}_1, \mathfrak{t}_1)$ and $\varphi(\mathfrak{s}_0, \mathfrak{t}_0)$, with given factorization, appear as equations (5) and (6), respectively, in Hisil et al. [11]. Similarly, in expanded form Corollary 43 gives the addition law projections of Bernstein and Lange [3]:

$$\begin{aligned}\mathfrak{s}_0 \circ \varphi \times \varphi &= (X_1 Y_1 Z_2 W_2 + Z_1 W_1 X_2 Y_2, a X_1 W_1 X_2 W_2 + Z_1 W_1 Z_2 W_2), \\ \mathfrak{s}_1 \circ \varphi \times \varphi &= (X_1 W_1 Z_2 Y_2 + Z_1 Y_1 X_2 W_1, d X_1 Y_1 X_2 Y_2 + Z_1 W_1 Z_2 W_2), \\ \mathfrak{t}_0 \circ \varphi \times \varphi &= (X_1 Y_1 Z_2 W_2 - Z_1 W_1 X_2 Y_2, X_1 W_1 Z_2 Y_2 - X_1 W_1 Z_2 Y_2), \\ \mathfrak{t}_1 \circ \varphi \times \varphi &= (a X_1 W_1 X_2 W_2 - Z_1 Y_1 Z_2 Y_2, d X_1 Y_1 X_2 Y_2 - Z_1 W_1 Z_2 W_2).\end{aligned}$$

The set of exceptional divisors of these addition laws, described in Bernstein and Lange [3, Section 8], is equivalent to that of Theorem 39, since the Segre embedding is globally defined by a single polynomial map with trivial exceptional divisor.

Canonical curve of level 4. In light of the simple structure of the twisted Hessian curve, we define a canonical model C/k of level n to be an elliptic curve with subgroup scheme $G \cong \mu_n$, embedded in \mathbb{P}^r for $r = n - 1$. Moreover we assume that there exists T in $G(k(\zeta))$, for an n -th root of unity ζ in \bar{k} , such that

$$\tau_T(X_0 : X_1 : \cdots : X_r) \longmapsto (X_0 : \zeta X_1 : \cdots : \zeta^r X_r).$$

Moreover, there exists S in $C(\bar{k})$ such that $\langle S, T \rangle = C[n]$ and for some a_0, \dots, a_r in \bar{k} ,

$$\tau_S(X_0 : X_1 : \cdots : X_r) \longmapsto (a_1 X_1 : \cdots : a_r X_r : a_0 X_0).$$

This generalizes the Hessian model and the diagonalized Edwards model (of the -1 twist).

The Edwards curve, with $a = 1$,

$$\begin{aligned}X_0^2 + dX_3^2 &= X_1^2 + X_2^2, \\ X_0 X_3 &= X_1 X_2,\end{aligned}$$

has 4-torsion point $S = (1 : 1 : 0 : 0)$ such that τ_S is:

$$\tau_S(X_0 : X_1 : X_2 : X_3) = (X_0 : X_2 : -X_1 : -X_3),$$

defined by the matrix

$$\begin{pmatrix} 1 & & & \\ & 0 & -1 & \\ & 1 & 0 & \\ & & & -1 \end{pmatrix}$$

which we wish to diagonalize. First we twist by $a = -1$ so that the diagonalization descends, and from the twisted Edwards curve, with $a = -1$,

$$X_0^2 - dX_3^2 = -(X_1 - X_2)(X_1 + X_2), \quad X_0 X_3 = X_1 X_2,$$

we find the *canonical curve C of level 4*:

$$\begin{aligned}X_0^2 - dX_2^2 &= X_1 X_3, \\ X_1^2 - X_3^2 &= 4X_0 X_2,\end{aligned}$$

via the isomorphism

$$(X_0 : X_1 : X_2 : X_3) \mapsto (X_0 : X_1 + X_2 : X_3 : -X_1 + X_2).$$

This curve has identity $(1 : 1 : 0 : 1)$ and the point $(i : 1 : 0 : 0)$ on E maps to $(1 : i : 0 : -i)$ on C , which acts by

$$(X_0 : X_1 : X_2 : X_3) \mapsto (X_0 : iX_1 : -X_2 : -iX_3).$$

Theorem 44 *The space of addition laws of bidegree $(2, 2)$ for the canonical model of level 4 is spanned by :*

$$\begin{aligned} \mathfrak{s}_0 = & \begin{pmatrix} -(X_1^2 Y_3^2 - X_3^2 Y_1^2)/4, \\ X_0 X_3 Y_1 Y_2 - X_1 X_2 Y_0 Y_3, \\ X_0^2 Y_2^2 - X_2^2 Y_0^2, \\ X_0 X_1 Y_2 Y_3 - X_2 X_3 Y_0 Y_1, \end{pmatrix} & \mathfrak{s}_1 = & \begin{pmatrix} X_0 X_1 Y_0 Y_3 + dX_2 X_3 Y_1 Y_2, \\ 4dX_0 X_2 Y_2^2 + X_1^2 Y_1 Y_3, \\ X_0 X_3 Y_2 Y_3 + X_1 X_2 Y_0 Y_1, \\ X_1 X_3 Y_3^2 - 4dX_2^2 Y_0 Y_2, \end{pmatrix} \\ \mathfrak{s}_2 = & \begin{pmatrix} X_0^2 Y_0^2 - d^2 X_2^2 Y_2^2, \\ X_0 X_1 Y_0 Y_1 - dX_2 X_3 Y_2 Y_3, \\ (X_1^2 Y_1^2 - X_3^2 Y_3^2)/4, \\ X_0 X_3 Y_0 Y_3 - dX_1 X_2 Y_1 Y_2, \end{pmatrix} & \mathfrak{s}_3 = & \begin{pmatrix} X_0 X_3 Y_0 Y_1 + dX_1 X_2 Y_2 Y_3, \\ X_1 X_3 Y_1^2 + 4dX_2^2 Y_0 Y_2, \\ X_0 X_1 Y_1 Y_2 + X_2 X_3 Y_0 Y_3, \\ -4dX_0 X_2 Y_2^2 + X_3^2 Y_1 Y_3. \end{pmatrix} \end{aligned}$$

8.3 Symmetric elliptic curve models of degree 5

In analogy with the Hessian model and canonical model of level 4, we describe the construction of a canonical model of level 5, which we call pentagonal elliptic curves. As with the canonical models of levels 3 and 4, the addition laws have simple expressions in terms of differences of monomials.

Pentagonal elliptic curves. We describe a model for elliptic curves over the function field $k(t)$ of $X_1(5)$. Let $E/k(t)$ be the elliptic curve in \mathbb{P}^4 defined by

$$\begin{aligned} tU_0^2 + U_2U_3 - U_1U_4 &= tU_0U_1 + U_2U_4 - U_3^2 = U_1^2 + U_0U_2 - U_3U_4 = 0 \\ U_1U_2 + U_0U_3 - U_4^2 &= U_2^2 - U_1U_3 + tU_0U_4 = 0, \end{aligned}$$

with base point $O = (0 : 1 : 1 : 1 : 1)$. This model is derived from an input Weierstrass model E over $k(t)$ by computing the Riemann-Roch space $\Gamma(E, \mathcal{L}(G))$ where $G = \langle T \rangle$ is a cyclic subgroup of order 5, considered as a divisor on E . The coordinate functions U_i are determined by a choice of basis of eigenfunctions for the translation-by- T map. For a 5-th root of unity ζ , the image of T is $(0 : \zeta : \zeta^2 : -\zeta^3 : -\zeta^4)$ and translation-by- T induces:

$$(U_0 : U_1 : U_2 : U_3 : U_4) \mapsto (U_0 : \zeta U_1 : \zeta^2 U_2 : \zeta^3 U_3 : \zeta^4 U_4).$$

We note that the projection to $(U_0 : U_1 : U_4)$ yields a plane model

$$U_1^5 + U_4^5 - (t-3)U_1^2U_4^2U_0 + (2t-1)U_1U_4U_0^3 - tU_0^5,$$

but that being singular the dimension formulas fail to apply. Indeed there are no bidegree $(2, 2)$ addition laws for this planar model.

Theorem 45 *The space of addition laws of bidegree $(2, 2)$ on E is of dimension 5 and decomposes over $k(t)$ into eigenspaces for the action of G_1 . The eigenspace for 1 is given by the polynomial maps:*

$$\begin{aligned} (U_0^2 V_1 V_4 - U_1 U_4 V_0^2 &= (U_1 U_4 V_2 V_3 - U_2 U_3 V_1 V_4)/t = -U_2 U_3 V_0^2 + U_0^2 V_2 V_3 : \\ U_0 U_1 V_2 V_4 - U_2 U_4 V_0 V_1 &= (-U_2 U_4 V_3^2 + U_3^2 V_2 V_4)/t = U_0 U_1 V_3^2 - U_3^2 V_0 V_1 : \\ U_0 U_2 V_3 V_4 - U_3 U_4 V_0 V_2 &= U_0 U_2 V_1^2 - U_1^2 V_2 V_0 = -U_1^2 V_3 V_4 + U_3 U_4 V_1^2 : \\ U_0 U_3 V_1 V_2 - U_1 U_2 V_0 V_3 &= U_0 U_3 V_4^2 - U_4^2 V_0 V_3 = -U_1 U_2 V_4^2 + U_4^2 V_1 V_2 : \\ U_0 U_4 V_1 V_3 - U_1 U_3 V_0 V_4 &= U_0 U_4 V_2^2 - U_2^2 V_0 V_4 = (U_1 U_3 V_2^2 - U_2^2 V_1 V_3)/t). \end{aligned}$$

Remark. The function t can be identified with a modular function generating the function field of $X_1(5)$. The modular curve $X(5)$ is also of genus 0, and there exists a modular function e satisfying $t = e^5$ which generates the function field of $X(5)$. Over this extension the 5-torsion point $S = (1 : e : -e^2 : e^3 : 0)$, and the translation-by- S morphism is:

$$(U_0 : U_1 : U_2 : U_3 : U_4) \mapsto (-U_4 : e^4 U_0 : e^3 U_1 : -e^2 U_2 : e U_3).$$

The remaining eigenspaces of addition laws are permuted by the action induced by the subgroup $G = \langle S \rangle$. In particular, since the action is a scaled monomial permutation, the remaining eigenspaces are also described by binomial biquadratic polynomials.

Acknowledgement. The author thanks Dan Bernstein and Tanja Lange for helpful discussions and motivation to undertake this study. Moreover this work benefited from discussion with Christophe Ritzenthaler, pointers from Marc Hindry, and comments from Steven Galbraith. Finally, the author thanks the various anonymous referees for careful reading and comments leading to an improvement of the article.

References

- [1] D. J. Bernstein, T. Lange. Faster addition and doubling on elliptic curves. *Advances in Cryptology: ASIACRYPT 2007*, Lecture Notes in Computer Science, **4833**, Springer, 29–50, 2007.
- [2] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters, Twisted Edwards curves. *Progress in cryptology – AFRICACRYPT 2008*, Lecture Notes in Computer Science, **5023**, 389–405, 2008.
- [3] D. J. Bernstein and T. Lange. A complete set of addition laws for incomplete Edwards curves, preprint, <http://eprint.iacr.org/2009/580>, 2009.
- [4] D. J. Bernstein, D. Kohel, and T. Lange. Twisted Hessian curves, preprint, 2010.
- [5] C. Birkenhake and H. Lange. *Complex abelian varieties*. Grundlehren der Mathematischen Wissenschaften, **302**, Springer-Verlag, 2004.

- [6] W. Bosma and H. W. Lenstra, Jr. Complete systems of two addition laws for elliptic curves. *J. Number Theory*, **53** (2), 229–240, 1995.
- [7] W. Castryck and F. Vercauteren. Toric forms of elliptic curves and their arithmetic. preprint 2010.
- [8] D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. in Appl. Math.*, **7**, (4), 385–434, 1986.
- [9] H. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, **44**, 393–422, 2007.
- [10] R. Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, **52**, Springer-Verlag, 1977.
- [11] H. Hisil, K. K.-H. Wong, G. Carter, E. Dawson, Twisted Edwards curves revisited, *Advances in cryptology – ASIACRYPT 2008*, Lecture Notes in Computer Science, **5350**, Springer, Berlin, 326–343, 2008.
- [12] H. Hisil, K. K.-H. Wong, G. Carter, E. Dawson, Faster group operations on elliptic curves, <http://eprint.iacr.org/2007/441>, 2007.
- [13] M. Joye and J.-J. Quisquater, Hessian elliptic curves and side-channel attacks. *Cryptographic hardware and embedded systems—CHES 2001 (Paris)*, Lecture Notes in Computer Science, **2162**, Springer, Berlin, 402–410, 2001.
- [14] D. Kohel et al., Echidna Algorithms (Version 2.0), <http://echidna.maths.usyd.edu.au/kohel/alg/index.html>, 2009.
- [15] S. Lang. *Abelian varieties*. Springer-Verlag, 1983.
- [16] H. Lange and W. Ruppert. Complete systems of addition laws on abelian varieties. *Invent. Math.*, **79** (3), 603–610, 1985.
- [17] H. Lange and W. Ruppert. Addition laws on elliptic curves in arbitrary characteristics, *J. Algebra*, **107**, 106–116, 1987.
- [18] Magma Computational Algebra System (Version 2.16), <http://magma.maths.usyd.edu.au/magma/handbook/>, 2010.
- [19] M. Monagan and R. Pierce. Rational simplification modulo a polynomial ideal. *ISSAC 2006*, 239–245, ACM, New York, 2006.
- [20] D. Mumford. *Abelian varieties*. Oxford University Press, 1970.
- [21] T. Sekiguchi, On projective normality of Abelian varieties, II. *J. Math. Soc. Japan*, **29** (1977), no. 4, 709–727.
- [22] N. Smart. The Hessian form of an elliptic curve. *Cryptographic hardware and embedded systems—CHES 2001 (Paris)*, 118–125, Lecture Notes in Computer Science, **2162**, Springer, Berlin, 2001.
- [23] W. A. Stein et al., Sage Mathematics Software (Version 4.3.5), The Sage Development Team, <http://www.sagemath.org>, 2010.